

UNITED STATES DISTRICT COURT

for the

Southern District of California

2014 APR 11 AM 10:28

MCB  
for  
JPM

~~SEALED~~  
UNSEALED

2/25/15

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

Google, Inc.

1065 La Avenida, Mountain View, CA

CLERK US DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA

Case No. \_\_\_\_\_

'14 MJ8324

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-4

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-4

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

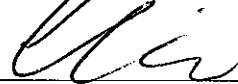
Code Section	Offense Description
18 USC 2320; 18 USC 1956;	Trafficking of counterfeit goods and services; money laundering; mail fraud; wire
18 USC 1341; 18 USC 1343;	fraud; tax evasion; and filing of false tax returns
26 USC 7201; 26 USC 7206	

The application is based on these facts:

REFER TO ATTACHED AFFIDAVIT OF HSI SPECIAL AGENT CHRISTIANSEN MADSEN

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



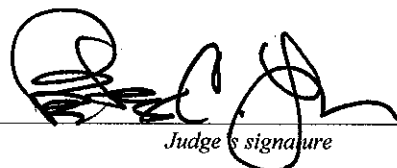
Applicant's signature

Christiansen Madsen, SA ICE, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 4-11-2014 @ 10:15 a.m.



Judge's signature

City and state: El Centro, CA

United States Magistrate Judge Peter C. Lewis

Printed name and title

① kcm

**ATTACHMENT A-4**

**Place to Be Searched**

Google, Inc. is an Internet Service Provider with its primary computer information systems and other electronic communications and storage systems, records and data located at 1600 Amphitheater Parkway, Mountain View, California 94043.

## **ATTACHMENT B-4**

### **I. Service of Warrant**

The officer executing the warrant shall permit Google, Inc. (the "ISP"), as custodian of the files described in Section II, to locate and copy them onto removable electronic storage media and deliver the same to the officer.

### **II. Data to Be Supplied by the ISP**

The ISP shall copy to electronic storage media all files [including emails, attachments, buddy lists, profiles, access logs, transactional data, billing records, and any other related financial, subscriber, and user records] associated with **octaviocesarsana@gmail.com** ("the subject account") for the period January 1, 2013 to the date this warrant is signed.

### **III. Search and Seizure of Data by Law Enforcement**

Law enforcement shall conduct any search of the data pursuant to the "Procedures For Electronically Stored Information" section of the affidavit supporting the search warrant. Law enforcement is authorized to seize data **limited to:**

- A. The purchase, sale, or shipment of counterfeit cellular phone parts or other counterfeit electronics;
- B. The resale of counterfeit cellular phone parts or other counterfeit electronics in the United States;
- C. The receipt or distribution of payments for counterfeit cellular phone parts or other counterfeit electronics; and
- D. The dominion and control of the subject account;

evidencing (1) trafficking in counterfeit goods in violation of 18 U.S.C. § 2320, (2) money laundering in violation of 18 U.S.C. § 1956, (3) mail fraud in violation of 18 U.S.C. § 1341, (4) wire fraud in violation of 18 U.S.C. § 1343, (5) tax evasion in violation of 26 U.S.C. § 7201, or (6) filing false returns in violation of 26 U.S.C. § 7206(1).

MCB  
for  
JPM

**AFFIDAVIT**

I, Christiansen C. Madsen, being duly sworn, state as follows:

**I. INTRODUCTION**

**A. Training and Experience**

1. I am a Special Agent with the U.S. Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") with the Department of Homeland Security ("DHS"). I have been so employed since January 3, 2010. Prior to my employment with ICE, I served as a United States Secret Service Uniformed Division Officer from October 2004 to January 2010.

2. I am a graduate of the Federal Law Enforcement Training Center ("FLETC"). At FLETC, I received training in criminal investigative techniques, including financial investigations, the execution of search warrants, and several other areas of law enforcement. Since becoming an agent, I have also received both formal and on-the-job training in the laws and regulations relating to the trafficking of counterfeit goods and services, money laundering, mail fraud, and wire fraud. I have also directed, and participated in, numerous investigations that involved these crimes. Additionally, I have worked with agents with the Internal Revenue Service ("IRS") who specialize in tax investigations. I have also led and/or participated in dozens of search warrants, including several electronic search warrants that targeted commercial fraud. I also communicate regularly with investigators with expertise in computers, computer forensics, and

least one brick-and-mortar store.

**C. Flexqueen Uses Online Merchant Services Account to Sell Counterfeit Goods**

7. Flexqueen's merchant services account records, which were obtained pursuant to the Flexqueen search, revealed that Flexqueen generated over \$3.5 million in revenue from nearly 30,000 sales through flexqueen.com over a five-year period from 2007-2012. Based on the larger investigation, which has included numerous undercover purchases of counterfeit goods and recorded conversations with Sana in which he discusses his sale of counterfeit goods, I believe most, if not all, of Flexqueen's business involves counterfeit items.

8. The Flexqueen search – and particularly a review of Flexqueen's merchant services account records – also identified over a dozen high-volume customers who operate throughout the United States. Typically, these businesses or individuals buy several thousands of dollars' worth of counterfeit cell phone parts and other electronics from Flexqueen on a regular basis (e.g., every month to two months).

9. Agents have confirmed that these customers are reselling the counterfeit parts they buy from Sana and Flexqueen. For instance, undercover officers made the following controlled purchases from several of Flexqueen's high-volume customers. In each instance, the items described below purchased by law enforcement were later confirmed as counterfeit by the respective, genuine manufacturer. Several of Flexqueen's high-volume customers admitted to knowing that the items they sold to

undercover officers (and believed to be obtained from Flexqueen) were, in fact, counterfeit.

- a. August 23, 2013: agents purchased two iPhone conversion kits (including LCD screen and back plate with Apple logo) and one iPhone back plate with Apple logo from a sales representative at GC Telecom, in Brownsville, Texas;
- b. September 4, 2013: agents purchased several iPhone parts that contained the Apple logo from "Tyson," a sales associate at Zoom Wireless, in Riverdale, Utah. During the controlled purchase, Nathan Bruce, aka "Michael," believed to be the store's owner, told agents that they get the parts from multiple manufacturers. Bruce explained that because some parts are "crap," a seller has to be "careful and choosy." Bruce noted to the officer that he had been taking the "risk" of importing and selling such counterfeit items for a long time;
- c. January 14, 2014: agents purchased three cell phone cases that contained the Apple logo from Young Taek Joe, aka, "Young Taek Yoe," an employee of Dream Wireless, in Doraville, Georgia. Young told officers that law enforcement is actively investigating the sale of "fake" parts. Young also explained that the quality of the "fake" parts can vary widely depending on the quality of the manufacturer in China;
- d. January 17, 2014: agents purchased 12 back plates for the iPhone 4S that

contained the Apple logo from Nagy Aziz, the manager of Cell Phone Doctors, in Nashville, Tennessee. Aziz described to officers that he had higher quality counterfeit goods than other suppliers;

- e. January, 21, 2014: agents purchased several iPhone parts that contained the Apple logo from Mohammad Ibrahim, owner of Magic Wireless, in Memphis, Tennessee. Ibrahim told officers, while referencing the fake iPhone parts, "I mean, we all know it's not Apple;"
- f. February 14, 2014: agents purchased iPhone 4 and 4S back plates that contained the Apple logo from Cornelius Blanc, the owner of Everything Cell Phone, in Orlando, Florida. Blanc told officers that "the Feds" are cracking down on counterfeit cell phone parts. During the order, Blanc called his vendor in California. Blanc told the vendor to give him the parts "the way you know I want it," which agents interpreted as a reference to attaching the Apple logo to the cell phone parts.
- g. February 27, 2014: agents purchased several iPhone parts that contained the word "Apple" and/or the Apple logo from multiple "WiGo Clinic" stores, in Fairfax, Virginia, owned by Rob Link;
- h. On March 8, 2014, agents purchased "Hello Kitty" back plates for iPhones that contained the Apple logo through an email to arifshah@msn.com, an email account associated with "Todo Wireless," a cell phone and electronics store in Chelsea, Massachusetts; and

- i. March 13, 2014: agents purchased an iPhone 4S conversion kit (including LCD screen and back plate with Apple logo) from Zehra Farooqui, owner of Cell Rite, in Saint Petersburg, Florida. During the sale, Farooqui's associate, Ramim Islam, told officers that they order their cell phone parts either from a supplier in California or directly from China. Email records show several purchases by Cell Rite from Flexqueen around this time.

10. Additionally, several of the high-volume purchasers from Flexqueen discussed selling counterfeit parts with undercover officers, even though they did not sell any to the officers. For example, on February 4, 2014, Gai Diep, aka "Guy," owner of multiple Millennium Trenz stores, in Colorado, told officers that he has "A+" quality products. I know from prior email records related to Sana and his former supplier in China, it is common for traffickers in counterfeit goods to grade different qualities of counterfeit items. Obviously, genuine manufacturers make, or at least attempt to make, a single quality of products. While Diep expressed reluctance to sell the undercover officer items with trademarked logos, he told the officer that he can order them. Flexqueen's merchant services records corroborate Diep's statement – records show Diep placed over 200 orders with Flexqueen for products that contained Apple, Blackberry, or other name brand logos.

11. Similarly, on February 10, 2014, Mickey Punjabi, a self-identified worker at Accessory Depot, in Saugus, Massachusetts, showed undercover officers counterfeit back



plates for iPhones (known to be counterfeit because they were in colors not available from Apple). Punjabi told officers they were available for \$8 apiece, which is significantly lower than an authentic Apple back plate, which cost \$39. At the end of the meeting, associates of Punjabi (believed to be his father) followed officers out of the store. When undercover officers later called to place their order, Punjabi was no longer willing to sell the counterfeit back plates. Punjabi said, "I am not an authorized Apple representative so I cannot sell you something that has an Apple logo on it." Punjabi explained that he did not want to jeopardize his business "for a few hundred bucks." When officers reminded Punjabi that they were willing to purchase the back plates they had seen for sale at his store, Punjabi told them that he did not want to sell the back plates to them.

12. Finally, on February 18, 2014, William H. Phillips, III, the owner of CCI Wireless, in Monroeville, Pennsylvania, told undercover officers that he gets his cell phone parts from "Flexqueen.com." Phillips further advised the undercover officer, who was posing as a fellow retailer of counterfeit goods, that the undercover officer should go directly to Flexqueen to purchase cell phone parts. Phillips continued, "Yeah, I buy all my back doors [iPhone back plates] from these guys because, I mean, they are not OEM [original equipment manufacturer], but I tell you what, their back doors, you put them up against an OEM, you can't hardly tell the difference." Email records show that CCI Wireless has made two recent purchases from flexqueen.com on December 26, 2013 and January 3, 2014.

13. Apple confirmed that none of the cell phone stores discussed above, including, Flexqueen, are approved vendors of Apple products.

14. Current email data shows that Flexqueen continues to use its merchant services account to track and process online sales of counterfeit cell phone parts and electronics, including to some customers described above. Email records show that when a customer places an order through Flexqueen's merchant services account, the website automatically generates an email to **admin@flexqueen.com**, which then automatically forwards the order to Sana's **amcellular@hotmail.com** account. The Flexqueen search revealed that Sana and associates use these two email accounts not only to process orders, but also to communicate with customers about their orders, including when customers identify flaws in the counterfeit items. For example, email records for **admin@flexqueen.com** and **amcellular@hotmail.com** show that the following orders were placed from customers (or their identified associates) discussed above:

- January 2, 2014 order from cellrite@gmail.com (under the name of Kiran Farooqui), which is believed to be related to the high-volume customer described in Paragraph 9.i., supra;
- January 3, 2014 order from billp@cci-wireless.com (under the name Randy Beltz), which is believed to be related to the high-volume customer described in Paragraph 12., supra;
- January 9, 2014 order from arifshah@msn.com (under the name Arif Shah,

identified as the owner of Todo Wireless), which is believed to be related to the high-volume customer described in Paragraph 9.h., supra; and

- January 21, 2014 order from rob@wigoclinic.com (under the name Rob Link), which is believed to be related to the high-volume customer described in Paragraph 9.g., supra .

**D. Other Emails Between Sana and Undercover Officers**

15. Sana provided his email account, **octaviocesarsana@gmail.com** to undercover officers in late 2013. Thereafter, Sana has used this account to email with undercover officers regarding his criminal activity. For example, on February 13, 2014, Sana emailed undercover officers to ask whether they were happy with a recent purchase of digitizer screens for the iPhone 5S. This order was the only undercover purchase made by officers in which the products were not labeled as Apple products. Apple investigators nonetheless confirmed with agents that the screens were not manufactured by Apple or an authorized manufacturer. Further, Apple investigators stated that, as of April 8, 2014, Apple has not even supplied iPhone 5s replacement parts to Apple Stores. Prior to this order, Sana told undercover officers that he no longer purchased digitizer screens for iPhones that were identified as Apple products because some of his prior orders had been seized (including three seizures related to this investigation).

16. Sana has also used this account to communicate with undercover officers about his Chinese sources of supply. For instance, in late 2013, agents discussed with

Sana arranging for Sana's supplier at the time, Hongwei Du (aka "Nick Du"), to come to the United States from China. The undercover officer, who purported to have contacts in law enforcement, had told Sana that he needed Du's biographical information in order to get Du a visa. Shortly thereafter, Sana emailed the undercover officer a photograph of Du's passport.

17. Sana has also used this account to arrange meetings with the undercover officer to discuss his counterfeit parts business. For example, on February 19, 2014, Sana emailed the officer to arrange a meeting that occurred on March 20, 2014. At the meeting, Sana told the officer he had a new counterfeit parts supplier. Sana also discussed future sales of counterfeit cell phone parts.

18. Finally, agents know from prior court-authorized searches that Sana uses this email account to communicate with coconspirators. For example, a search of Du's email account, duhongwei88@hotmail.com, showed numerous emails with Sana's Gmail account in which the two discussed the purchase and sale of counterfeit goods and in which Du provided Sana invoices for various shipments. Additionally, Du sent several of these emails to Sana's amcellular@hotmail.com account.

### **C. Target Subjects' Retention of Emails**

19. Based on my training and experience, I know that individuals who utilize emails in furtherance of their criminal activities tend to retain such emails for a long time. This is particularly true of individuals involved in commercial fraud, like here. As explained above, Sana and others associated with Flexqueen rely on their email

communications to buy and sell counterfeit electronics parts. Because of how they use email, it is common for them to retain emails related to their commercial transactions in order to maintain business records of their sales. In fact, agents know from prior searches of Sana's email accounts (including **amcellular@hotmail.com**) that he rarely, if ever, deletes business-related emails. Moreover, Sana has shown little concern for law enforcement detection, which results in him having little cause to delete incriminating emails. In fact, Sana has told undercover officers that he is not concerned with law enforcement and plans to "play dumb" if ever confronted by the authorities. Sana has also told undercover officers that he feels particularly secure because he has moved his records from hard copy to electronic cloud servers, which agents interpret to be a reference to his online merchant services account to be searched pursuant to the requested warrant. These factors, along with my training and experience, cause me to believe that Sana and others retain relevant emails in the accounts to be searched for long periods of time.

### **III. THE INTERNET SERVICE PROVIDERS**

20. YAHOO!, Inc., Microsoft, Inc., and Google, Inc. are ISPs that, among other things, provides electronic communication services to subscribers. The ISPs' electronic mail services allow subscribers to communicate with other subscribers and with others through the Internet. The ISPs' subscribers access subscriber services through the Internet.

21. The ISPs' subscribers use screen names during communications with others. The screen names may or may not identify the real name of the person using a particular screen name.

22. At the creation of an account with the ISP and for each subsequent access to the account, the ISP typically logs the Internet Protocol (IP) address of the computer accessing the account. An IP address is a unique address through which a computer connects to the Internet. IP addresses are leased to businesses and individuals by ISPs. Obtaining the IP addresses that have accessed a particular ISP account often identifies the ISP that owns and has leased that address to its customer. Subscriber information for that customer then can be obtained using appropriate legal process.

23. Based on the Flexqueen search, my conversations with YAHOO! representatives, and my training and experience, I know that portions of websites are not accessible to the public. Such protected areas of the websites are typically only accessible with "administrative rights." For merchant websites like flexqueen.com, all business records (e.g., merchant services account) are usually located in the administrative rights section.

24. Representatives from YAHOO! provided me with other general information about the use of merchant websites like flexqueen.com. According to YAHOO!, customers like Flexqueen/Ocesa Manufacturing essentially rent computer server space (commonly referred to as a "cloud" server) from YAHOO! in order to operate a website. YAHOO! confirmed that the non-public areas are restricted to administrators as

determined by the subscribers to the website. Thus, a subscriber can grant certain individuals different degrees of administrative access privileges. YAHOO! informed me that the non-public portions of merchant websites like flexqueen.com will contain all records of transactions conducted through the website and “merchant account providers.” According to YAHOO!, a merchant account provider is a third-party service provider that processes credit card transactions over a merchant website like flexqueen.com. YAHOO! indicated that their hosted merchant websites contain information regarding the merchant account provider utilized by the given website.

#### **IV. PROCEDURES FOR ELECTRONICALLY-STORED INFORMATION**

25. Federal agents and investigative support personnel are trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of the ISPs are not. It would be inappropriate and impractical for federal agents to search the vast computer network of the ISPs for the relevant accounts and then to analyze the contents of those accounts on the ISPs’ premises. The impact on the ISPs’ business would be severe.

26. Therefore, I request authority to seize all content as described in Attachment B-1 – B-4. In order to accomplish the objectives of the search warrants with a minimum of interference with the business activities of the ISPs, to protect the rights of the subject(s) of the investigation and to effectively pursue this investigation, authority is sought to allow the ISPs to make digital copies of the entire contents of the accounts subject to seizure. Those copies will be provided to me or to any authorized federal

agent. The copies will be forensically imaged and the image will then be analyzed to identify communications and other data subject to seizure pursuant to Attachment B-1 – B-4. Relevant data will be copied to separate media. The original media will be sealed and maintained to establish authenticity, if necessary.

27. Analyzing the data to be provided by the ISPs may require special technical skills, equipment and software. It also can be very time-consuming. Searching by keywords, for example, often yields many thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrants. Merely finding a relevant hit does not end the review process. Certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications, which files may have been attached to electronic mail, do not store data as searchable text. The data is saved in a proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases dramatically.

28. Based on the foregoing, searching the recovered data for the information subject to seizure pursuant to these warrants may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. The personnel conducting the examination will complete the analysis within ninety (90) days of receipt of the data from the service provider, absent further application to this court.



29. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize all electronic mails that identify any users of the subject accounts and any electronic mails sent or received in temporal proximity to incriminating electronic mails that provide context to the incriminating mails.

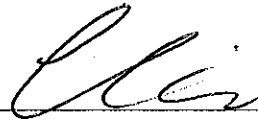
30. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of these warrants.

**V. REQUEST FOR SEALING AND PRECLUSION OF NOTICE**

31. This is an ongoing investigation of which the targets are unaware. It is very likely, based upon the above, that evidence of the crimes under investigation exists on ISPs' server space subject to the control of the targets. There is reason to believe, based on the above, that premature disclosure of the existence of the warrants will result in destruction or tampering with that evidence and seriously jeopardize the success of the investigation. Accordingly, it is requested that the warrants and all related materials be sealed until further order of the Court. In addition, pursuant to Title 18, United States Code, Section 2705(b), it is requested that this Court order the ISPs to whom these warrants are directed not to notify anyone of the existence of the warrants, other than its personnel essential to compliance with the execution of these warrants until further order of the Court.

## VI. CONCLUSION

32. Based on the foregoing, I believe probable cause exists to believe that the items in Attachments B-1 – B-4 constitute evidence of violations of trafficking of counterfeit goods and services (18 U.S.C. § 2320), money laundering (18 U.S.C. § 1956), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), tax evasion (26 U.S.C. § 7201), and filing of false returns (26 U.S.C. § 7206(1)) and that such items will be found at the locations to be searched as described in Attachments A-1 – A-4.



Christiansen Madsen, Special Agent  
Homeland Security Investigations

Subscribed to and sworn before me on this 11<sup>th</sup> day of April, 2014.



HONORABLE PETER C. LEWIS  
United States Magistrate Judge